Sicurezza, Firma Digitale e Licenze Software

Prof. Francesco Moscato
Seconda Università di Napoli
francesco.moscato@unina2.it

Outline

- Problemi di Sicurezza
- Obiettivi dei sistemi di sicurezza
- Autenticazione, Riservatezza, Autorizzazione, Integrità, Non ripudio, Disponibilità
- Crittografia e firma digitale
- Firma Digitale: aspetti metodologici-architetturali
- Firma Digitale: aspetti giuridici
- Licenze Software
- GPL
- BDS
- Creative Commons

Sicurezza

- Problemi da Affontare:
  - **Confidenzialità**: Occultamento di **informazioni** a chi non è *autorizzato*.
    - Contenuto dei Dati (crittografia)
    - Esistenza dei Dati (hiding, politiche di accesso ai dati)
  - **Integrità**: I **dati** non sono stati alterati (fiducia nei dati)
    - Integrità dei dati
    - Integrità della sorgente (autenticazione)
  - **Disponibilità**: Possibilità di usare informazioni e risorse richieste.

Minacce alla Sicurezza

- **Discolsure** (rivelazione)
  - Accesso non autorizzato ad una informazione
- **Deception** (raggiro, frode)
  - Accettazione di dati falsi
  - Accettazione da parte di una identità usurpata
- **Disruption** (rottura)
  - Interruzione o Prevenzione di un'operazione corretta
- **Usurpation** (usurpazione)
  - Controllo non autorizzato di Parti del SIstema

Necessità

- **Riservatezza**:
  - la comunicazione è stata intercettata?
- **Autenticazione**:
  - l'utente è veramente chi dice di essere?
- **Autorizzazione**:
  - ogni utente può accedere solo alle risorse cui ha diritto.
- **Integrità**:
  - i dati ricevuti (trattati) sono proprio quelli spediti (originali)?
- **Non ripudio**:
  - il mio interlocutore può ritrattare quello che ha detto?
- **Disponibilità**:
  - il mezzo di comunicazione o si servizi sono stati resi inutilizzabile?

Crittografia

- Risponde alle necessità prima esposte
- Una pratica antica
  - Egiziani, Romani...
- Dato una **informazione** contenuta in un **dato**, la cui **codifica** è nota, si utilizza una nuova **codifica** la cui interpretazione è associata ad una **chiave** “segreta” (cifratura)
  - Es: il messaggio “attaccate al tramonto” i cui dati sono la sequenza di caratteri del nostro alfabeto, a cui è associata l'informazione di attaccare al tramonto, potrebbe essere codificata nel seguente modo:
    - “buubddbuf bm usbnpoup” (la chiave di codifica è: lettera seguente dell'alfabeto, la chiave di decodifica è lettera precedente dell'alfabeto)
  - La codifica è semplice ma **anche la decodifica** lo è

Crittografia: Necessità

- Perché un sistema di crittografia sia **efficace**, è necessario che un dato crittografato sia
  - **Impossibile o**
    - (bisogna dimostrarlo matematicamente)
  - **Estremamente complicato**
    - In termini di tempo e costo della decodifica (bisogna dimostrarlo matematicamente)
- da decodificare **se non si conosce la chiave di decodifica**
- **NOTA:** non è detto che la chiave di codifica e decodifica siano le stesse...
  - Nel caso del messaggio precedente, la chiave era la stessa ed era il numero 1
    - L'algoritmo di codifica sostituiva ad ogni lettera la successiva
    - L'algoritmo di decodifica sostituiva ad ogni lettera la precedente

Obiettivi di un sistema di sicurezza

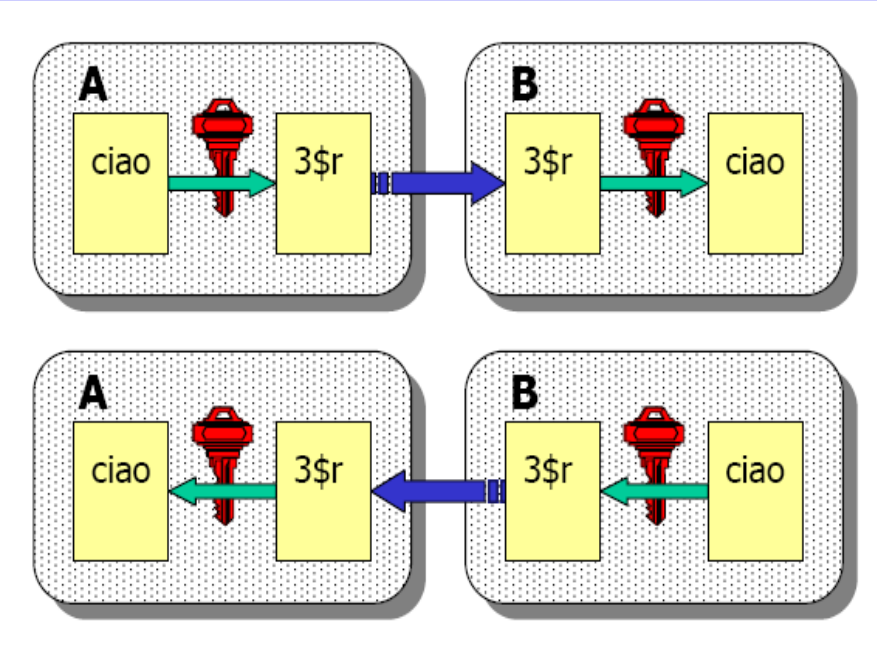
- Prevention (prevenzione)
  - Evitare gli attacchi alla sicurezza PRIMA che questi avvengano (terminino) con successo
    - Es: un firewall che identifica gli attacchi MENTRE avvengono
    - Es: un dato crittografato
- Detection (individuazione)
  - Individuare gli effetti degli attacchi dopo che questi sono stati effettuati con successo
- Recovery (ripristino)
  - Ripristino del sistema in uno stato **sicuro**

Riservatezza: Cifratura

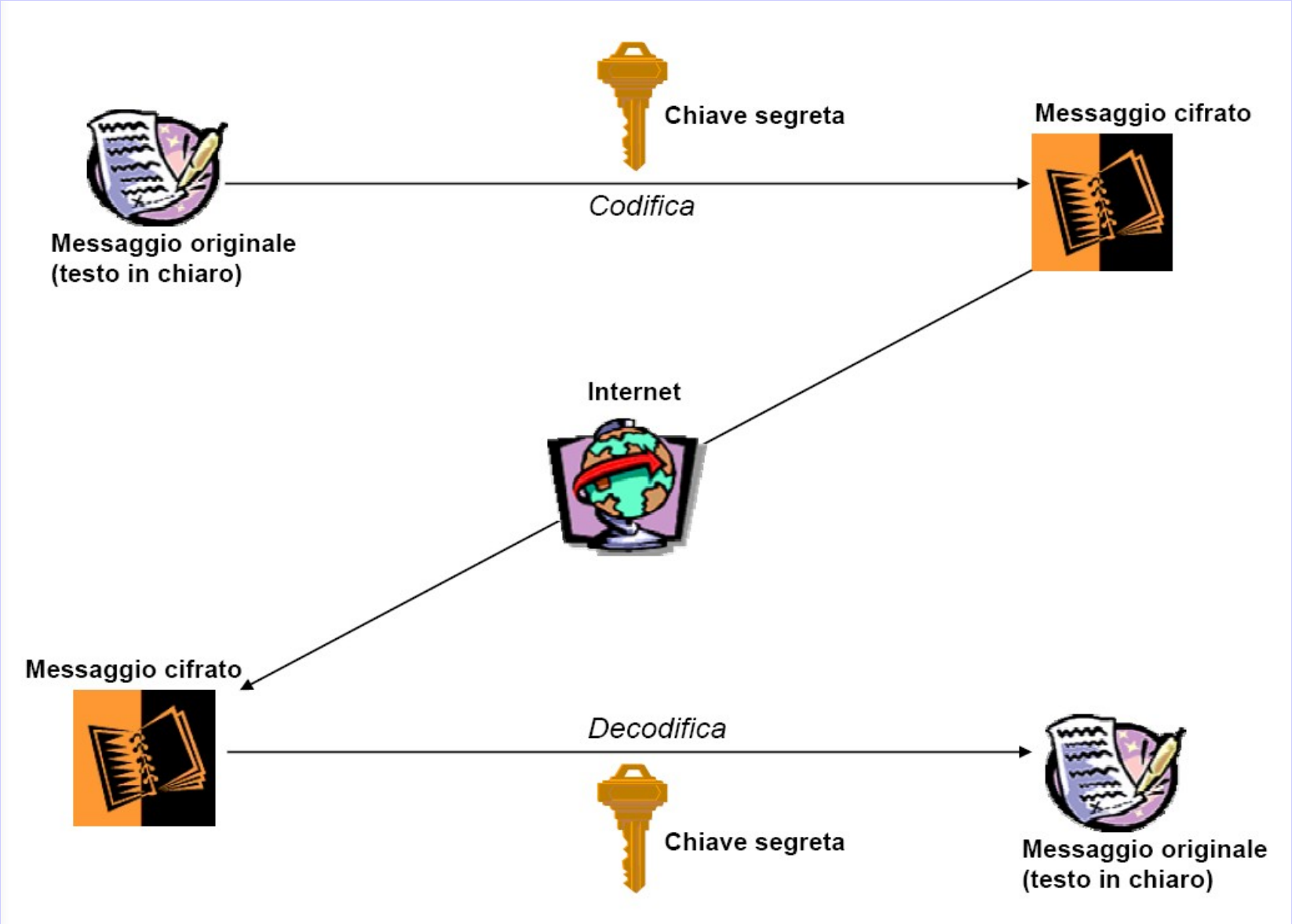
- Scegliere l'algoritmo per la codifica (**cifratura**)/decodifica (**decifratura**)
  - Due Principali categorie:
    - Chiave Simmetrica: stessa chiave per codifica e decodifica
    - Chiave Asimmetrica: chiavi diverse per codifica e decodifica
- Scegliere il tipo di Chiave
  - Legata a uno o più di questi 3 criteri
    - What you have: smartcard, badge magnetico, una chiave...
    - What you know: password, pin, utente e password ...
    - What you are: impronta digitale, impronta della retina ...
- Scegliere come distribuire e gestire le chiavi
  - CA
  - PKI
  - ...

Chiave Simmetrica

- Una chiave segreta nota ai corrispondenti
- La stessa chiave serve a cifrare e decifrare il messaggio
- Sia il “mittente” che il “ricevente” condividono la **stessa** chiave segreta
- Pro
  - Veloce (computazionalmente)
- Contro
  - Se le entità che devono comunicare sono **n**, le chiavi sono dell'ordine di **n*n**
    - Una chiave diversa per ogni destinatario
  - Non vi è garanzia di **univocità** e **autenticità** del mittente

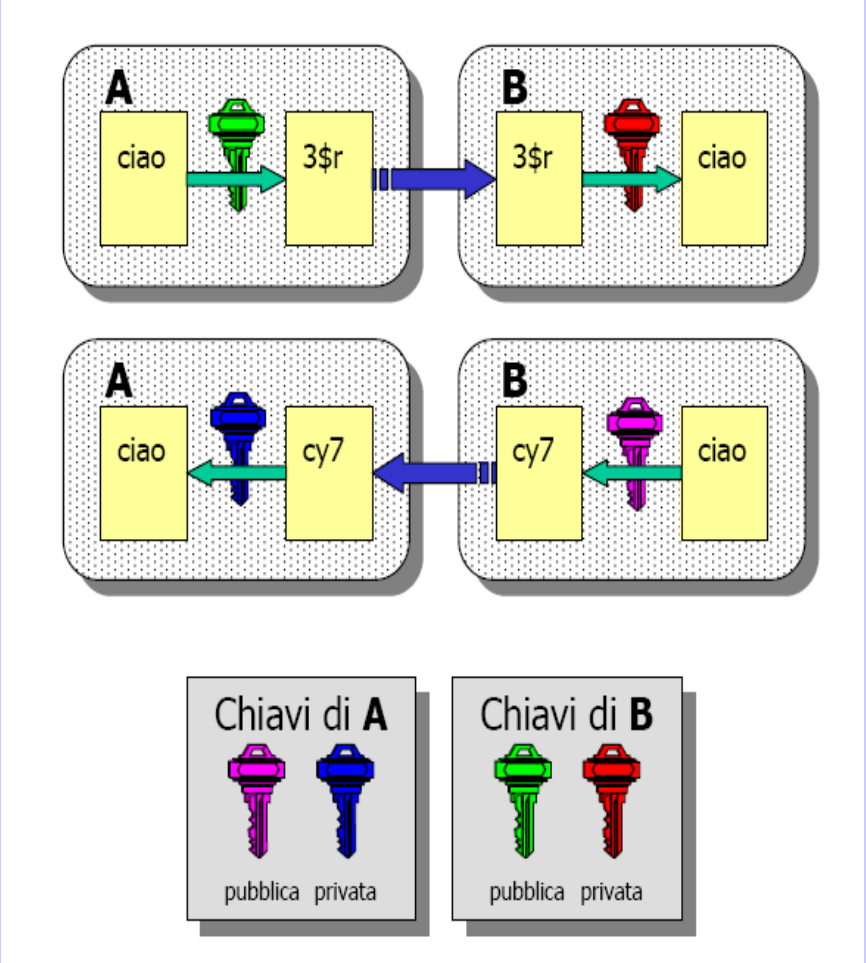


Chiave Simmetrica

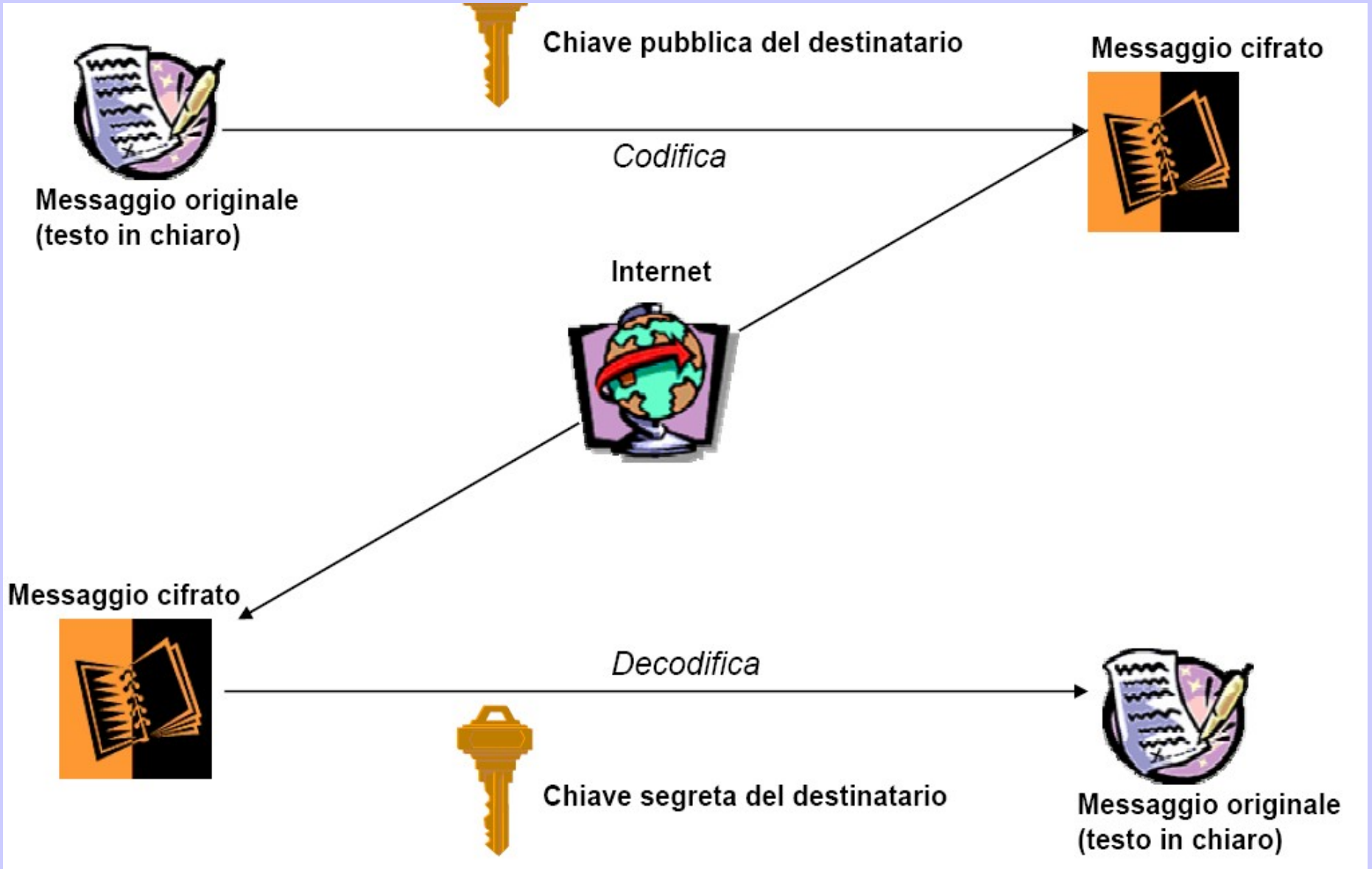


Chiave Asimmetrica

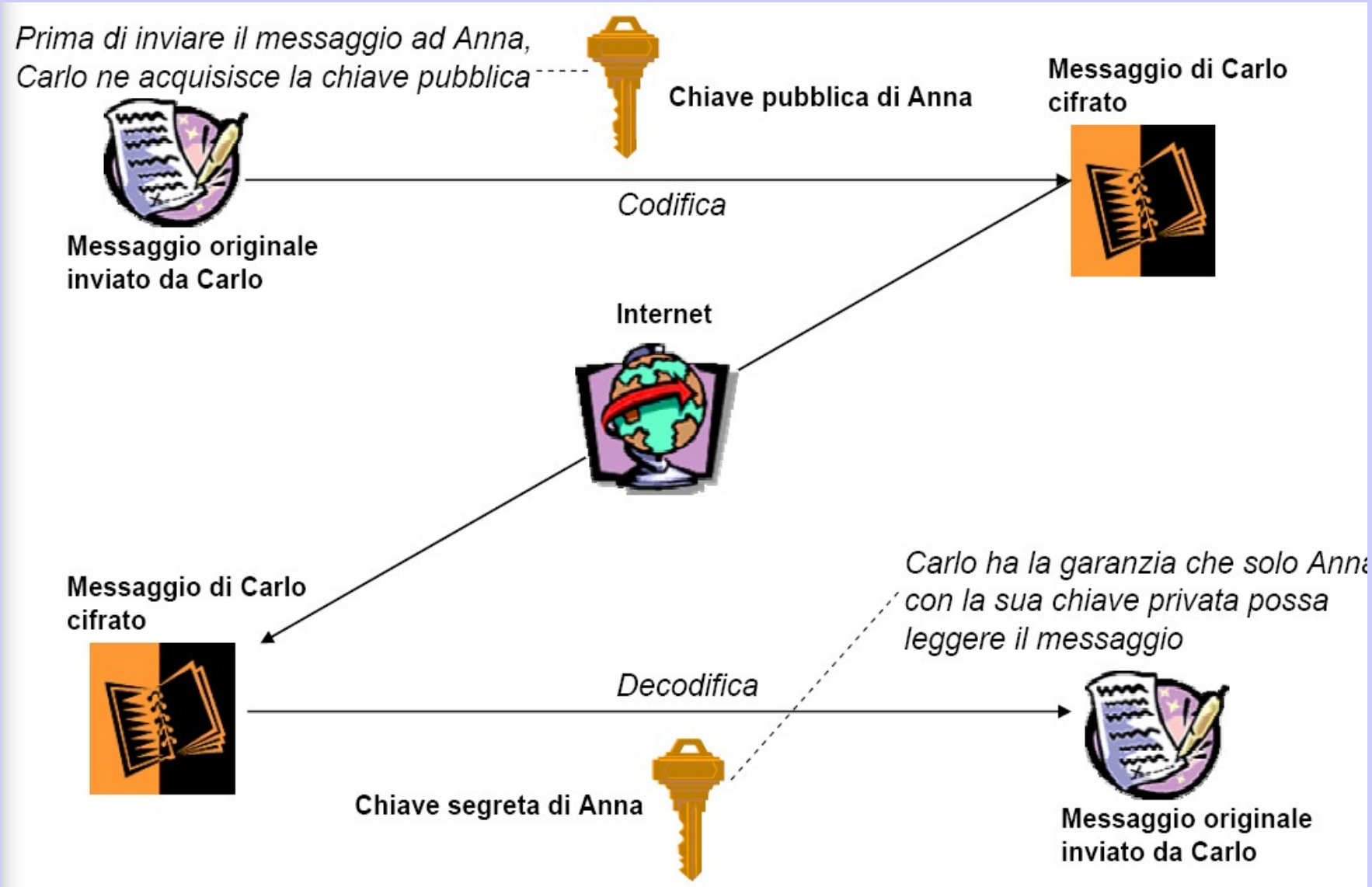
- Crittografia a **chiave pubblica**
- Ogni utente ha 2 chiavi: **una privata** e **una pubblica**
- Dalla chiave pubblica è **praticamente impossibile** ricavare quella privata
- La **cifratura** prodotta con una delle due chiavi può essere **decifrata** solo dall'altra chiave
  - Cifratura con chiave pubblica, decifratura con chiave privata
    - Cifratura
  - Cifratura con chiave privata, decifratura con chiave pubblica
    - Firma Digitale
- Un Algoritmo largamente utilizzato:
  - RSA
  - L'algoritmo crittografico è pubblico
  - Il punto di forza è la segretezza delle chiavi e l'impossibilità di ricavare la chiave pubblica da quella privata



Chiave Asimmetrica



Chiave Asimmetrica: Confidenzialità



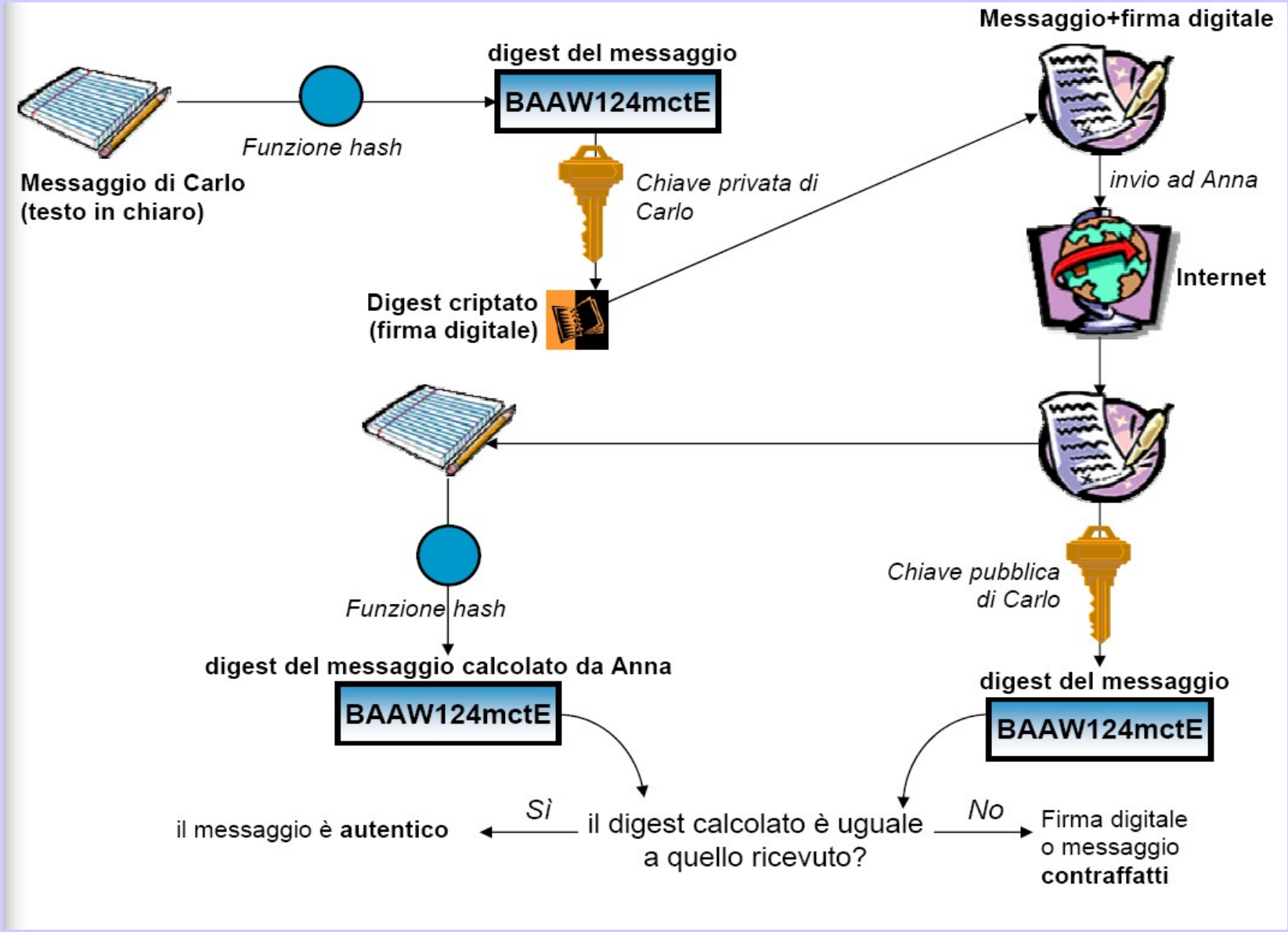
Chiave Asimmetrica: Firma Digitale

- Gli algoritmi a chiave asimmetrica sono computazionalmente più complessi di quelli a chiave simmetrica
- Perchè sia valida a norma di legge
  - La Firma deve essere immagazzinata su dispositivi appropriati (smartcard) difficili da crackare
  - La codifica e la decodifica devono essere fatta direttamente sulla smartcard (che ha un processore, una memoria etc.) tramite appositi lettori
    - Un dispositivo embedded
    - Risorse limitate
    - Non si può pensare di codificare e decodificare file di enormi dimensioni:
      - Funzioni di Hash

Hash (Integrità, firma e non ripudio)

- Le funzioni di Hash risolvono il problema dell'integrità
  - Sono funzioni (H) che hanno in ingresso un messaggio (M) di dimensioni **variabili** e producono un messaggio in uscita (**digest**) di dimensioni **FISSE**(in genere centinaia di byte)
    - Dato il messaggio deve essere *facile* produrre il digest
    - Dato il digest deve essere *difficile* risalire al messaggio generatore
  - Alcuni algoritmi: SHA, MD5,...
  - Utilizzato nella firma digitale permette di firmare solo il Digest (piccolo)
- Controllo dell'integrità:
  - Ad ogni Documento si associa il suo Digest.
  - Il Digest si protegge (crittografia)
  - Quando si distribuisce il documento, si distribuisce anche suo il Digest
  - In ricezione si calcola il Digest del messaggio ricevuto e si confronta con quello prodotto dalla sorgente
  - Se cambia anche un solo Bit nel Messaggio originale, i digest non corrispondono (e quindi il messaggio originale è stato manomesso)

Firma Digitale

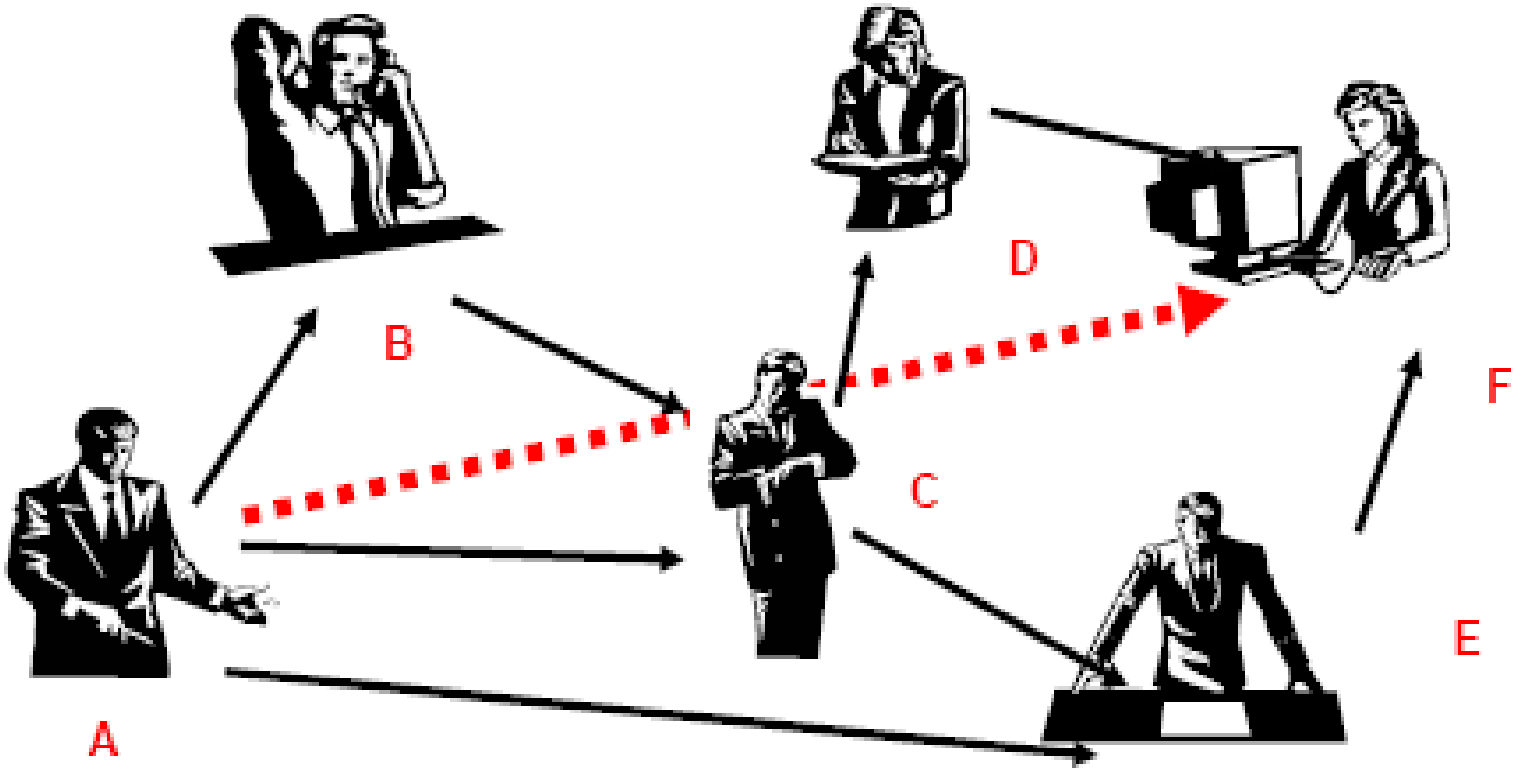


Firma Digitale

Autenticazione: Certificati

- La firma digitale rende sicuro un messaggio se:
  - La chiave privata di A non è stata compromessa
  - B è in possesso della chiave pubblica di A
    - Come può essere certo B di possedere la **vera** chiave di A?
- E' necessario convalidare l'abbinamento tra dati anagrafici e chiavi pubbliche
  - **Certificati digitali**
  - Autorità che gestiscano i certificati e le autenticità delle chiavi pubbliche (**Certification Authority**)
  - A e B devono **fidarsi** della CA
- Modelli principali di CA
  - PGP: Web of Trust
  - X.509: organizzazione gerarchica

PGP



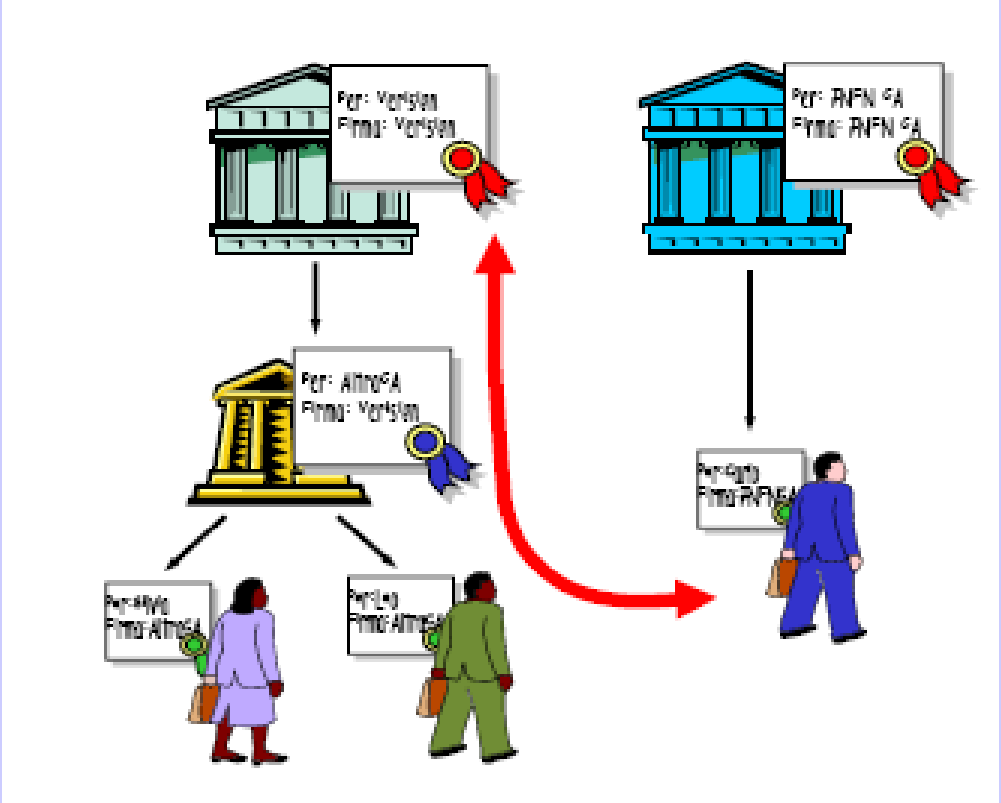
- F conosce D e E, che conosce A e C, che conosce A e B.
- F è ragionevolmente sicura che la chiave provenga da A.

Certificati X.509

- Certificato
  - Informazioni sul proprietario
  - Data di Scadenza
  - Chiave pubblica del proprietario
  - Informazioni sul garante (CA)
  - Firma della CA
- I Certificati sono pubblicate su directory pubbliche
  - WWW
  - LDAP
  - ...
- Possono essere Revocati
  - Es: si smarrisce la smartcard con la chiave privata...
  - **Certificate Revocation List (CRL)**

Catene di CA

- Anche le CA hanno un proprio certificato
- Una CA può garantire che altre CA di livello inferiore siano fidate (root CA)
  - La root CA si Auto-Firma



Firme Elettroniche: Discipline Giuridiche e norme elettroniche

- Gestite dal CNIPA (www.cnipa.it)
- Firma elettronica (semplice?)
- Firma elettronica avanzata
- Firma elettronica sicura
- Firma elettronica qualificata
- Firma digitale

Codice dell'Amministrazione Digitale

- **firma elettronica** – l'insieme dei dati in forma elettronica, **allegati oppure connessi tramite associazione logica** ad altri dati elettronici, utilizzati come metodo di **autenticazione informatica**
- **firma elettronica qualificata** - la firma elettronica ottenuta attraverso una procedura informatica che garantisce **la connessione univoca al firmatario e la sua univoca autenticazione informatica**, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica
- **firma digitale** - un **particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche,** una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

Codice dell'Amministrazione Digitale

- Decreto Legislativo 04.04.2006 n. 159
- Art. 20 (Documento informatico)
- 1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti a tutti gli effetti di legge, agli effetti di legge, ai sensi delle disposizioni del presente codice.
- 1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di **qualità, sicurezza, integrità ed immodificabilità**, fermo restando quanto disposto dal comma 2.

Codice dell'Amministrazione Digitale

- 2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore e l'integrità del documento.
- 2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile

Codice dell'amministrazione digitale

- Art. 21 (Valore probatorio del documento informatico sottoscritto)
- 1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
- 2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria . (…)

Licenze del Software

- Il Software è un prodotto commerciale ma:
  - Nella maggior parte dei casi viene associata ad una **idea**
    - Es: il modo con cui è stato risolto il problema di sommare due numeri con la MdT
      - L'algoritmo (codificato nella tabella dalla MdT) è nata da una nostra idea ma:
      - Cosa ci permette di dire che quell'idea è solo nostra ?
      - Lo stesso algoritmo potrebbe essere stato pensato da chiunque altro
      - Come si fa a dire quando sia nata un'idea ? Chi è stato il primo ad averla ?
- Il Software non si vende!
  - Si permette l'utilizzo delle sue funzionalità (Licenza d'uso)
  - Il Software è sempre di proprietà di chi l'ha prodotto
    - A meno che questi non ne ceda i diritti di distribuzione e copia
    - A meno che questi non ne ceda (in alcuni paesi) la *proprietà intellettuale*

Licenze d'uso del Software

- Licenze d'uso a pagamento
  - La maggior parte dei prodotti commerciali
  - Licenze Temporanee
  - Licenze Node Locked
  - Licenze per gruppi di calcolatori o utenti
  - In genere non esiste la possibilità di duplicare, modificare e ridistribuire il SW
- Licenze Shareware
  - Il software viene distribuito gratuitamente in una versione con funzionalità limitate o con una licenza temporanea. In caso contrario occorre
- Licenze Freeware
  - Il software viene distribuito gratuitamente (spesso limitando l'utilizzo al di fuori del privato)
- Licenze Open Source
  - Il software viene distribuito gratuitamente Assieme al suo codice sorgente (il programma)

Licenze Libere: GPL

- Buona parte del software libero viene distribuito con la licenza **GNU GPL (GNU General Public License)**, scritta da **Richard Stallman** e **Eben Moglen** per garantire legalmente a tutti gli utenti le quattro libertà fondamentali.
- Dal punto di vista dello sviluppo software, la licenza GPL viene considerata una delle più restrittive, poiché impone che necessariamente ogni prodotto software derivato - ovvero, che modifica o usa codice sotto GPL - venga a sua volta distribuito con la stessa licenza.

Licenza GPL

- Il testo della GNU GPL è disponibile per chiunque riceva una copia di un software coperto da questa licenza. I licenziatari (da qui in poi indicati come "utenti") che accettano le sue condizioni hanno la possibilità di modificare il software, di copiarlo e ridistribuirlo con o senza modifiche, sia gratuitamente sia a pagamento. Quest'ultimo punto distingue la GNU GPL dalle licenze che proibiscono la ridistribuzione commerciale.
- Se l'utente distribuisce copie del software, deve rendere disponibile il codice sorgente a ogni acquirente, incluse tutte le modifiche eventualmente effettuate (questa caratteristica è detta copyleft). Nella pratica, i programmi sotto GNU GPL vengono spesso distribuiti allegando il loro codice sorgente, anche se la licenza non lo richiede. Ci sono casi in cui viene distribuito solo il codice sorgente, lasciando all'utente il compito di compilarlo.

Licenza GPL

- L'utente è tenuto a rendere disponibile il codice sorgente solo alle persone che hanno ricevuto da lui la copia del programma o, in alternativa, accompagnare il software con una offerta scritta di rendere disponibile il sorgente su richiesta e per il solo costo della copia. Questo significa, ad esempio, che è possibile creare versioni private di un software sotto GNU GPL, a patto che tale versione non venga distribuita a qualcun altro. Questo accade quando l'utente crea delle modifiche private al software ma non lo distribuisce: in questo caso non è tenuto a rendere pubbliche le modifiche.

Licenza GPL

- Dato che il software è protetto da copyright, l'utente non ha altro diritto di modifica o ridistribuzione al di fuori dalle condizioni di copyleft. In ogni caso, l'utente deve accettare i termini della GNU GPL solo se desidera esercitare diritti normalmente non contemplati dalla legge sul copyright, come la ridistribuzione. Al contrario, se qualcuno distribuisce un software (in particolare, versioni modificate) senza rendere disponibile il codice sorgente o violando in altro modo la licenza, può essere denunciato dall'autore originale secondo le stesse leggi sul copyright. È un intelligente cavillo legale, ed è per questo che la GNU GPL è stata descritta come un "copyright hack". La licenza specifica anche che il diritto illimitato di ridistribuzione non è garantito, in quanto potrebbero essere trovate delle debolezze legali (o "bug") all'interno della definizione di copyleft.

Licenze Libere: LGPL

- Una licenza simile, ma meno restrittiva, è la **GNU LGPL (GNU Lesser General Public License)**, che permette di utilizzare il codice anche in software proprietari e sotto altre licenze open source, purché le parti coperte da LGPL - anche se modificate - vengano comunque distribuite sotto la medesima licenza. In genere è utilizzata per librerie software.

Licenza BSD

- Il testo della licenza è considerato di pubblico dominio e può quindi essere modificato senza restrizioni

```
* Copyright (c) <year>, <copyright holder>
* All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions are met:
*     * Redistributions of source code must retain the above copyright
*       notice, this list of conditions and the following disclaimer.
*     * Redistributions in binary form must reproduce the above copyright
*       notice, this list of conditions and the following disclaimer in the
*       documentation and/or other materials provided with the distribution.
*     * Neither the name of the <organization> nor the
*       names of its contributors may be used to endorse or promote products
*       derived from this software without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY <copyright holder> ``AS IS'' AND ANY
* EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
* DISCLAIMED. IN NO EVENT SHALL <copyright holder> BE LIABLE FOR ANY
* DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
* (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
* SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

Licenza BSD

- Le licenze BSD garantiscono le quattro libertà del software e sono quindi qualificate come licenze per il software libero. Tuttavia risultando più aperte e libere di altre, ad esempio della licenza GNU General Public License (GNU GPL), non hanno fra i propri obiettivi quello di proteggere la libertà del software cui sono applicate ma semplicemente di rendere per tutti il software completamente libero, accessibile e modificabile. Chi infatti modifichi un programma protetto da licenze BSD, può ridistribuirlo usando la stessa o altra qualunque licenza e senza avere l'obbligo di redistribuire le modifiche apportate al codice sorgente. Per questo molti esponenti del movimento GNU, a cominciare da Richard Stallman suo fondatore, consigliano di non utilizzarle per poter meglio tutelare i proprietari con una licenza aperta ma più restrittiva come quella di Free Software Foundation.

Licenze BDS

- Le licenze BSD riflettono l'idea più ampia possibile del dono liberale: chiunque può fare ciò che meglio crede del programma rilasciato ed acquisito con l'unico dovere di citare l'autore (l'università di Berkeley); questo significa anche che chiunque può sviluppare in forma chiusa con una licenza proprietaria un programma BSD modificato, magari anche impedendo ai propri acquirenti di modificarlo e ridistribuirlo a loro volta.
- Es: MacOSX utilizza il sistema operativo FreeBSD

Licenze Creative Commons

- Licenze Creative Commons è la denominazione di alcune licenze di diritto d'autore rilasciate a partire dal 16 dicembre 2002 dalla Creative Commons, una società non-profit statunitense fondata nel 2001.
- Le licenze Creative Commons (attualmente alla versione 3.0) si ottengono combinando tra loro le seguenti quattro condizioni:
  - Attribuzione
    - Permette che altri copino, distribuiscano, mostrino ed eseguano copie dell'opera e dei lavori derivati da questa a patto che vengano mantenute le indicazioni di chi è l'autore dell'opera.
  - Non Commerciale
    - Permette che altri copino, distribuiscano, mostrino ed eseguano copie dell'opera e dei lavori derivati da questa solo per scopi di natura non commerciale.
  - Non Opere Derivate
    - Permette che altri copino, distribuiscano, mostrino ed eseguano soltanto copie identiche dell'opera; non sono ammessi lavori che derivano dall'opera o basati su di essa.
  - Condividi allo stesso modo
    - Permette che altri distribuiscano lavori derivati dall'opera solo con una licenza identica a quella concessa con l'opera originale.

Licenze Creative Commons

- La combinazione di queste 4 proprietà permette la creazione di 6 Licenze diverse
  - Attribuzione - Non Commerciale - Non Opere Derivate
  - Attribuzione - Non Commerciale - Condividi allo stesso modo
  - Attribuzione - Non Commerciale
  - Attribuzione - Non Opere Derivate
  - Attribuzione - Condividi allo stesso modo
  - Attribuzione